BRADLEY/GROMBACHER, LLP
Marcus J. Bradley, Esq. (SBN 174156)
Kiley L. Grombacher, Esq. (SBN 245960)
Lirit A. King, Esq. (SBN 252521)
31365 Oak Crest Drive, Suite 240
Westlake Village, California 91361
Telephone: (805) 270-7100
Facsimile: (805) 270-7589
E-Mail: mbradley@bradleygrombacher.com
kgrombacher@bradleygrombacher.com
lking@bradleygrombacher.com

Attorneys for Plaintiffs

(Additional counsel listed on following page)

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

JUAN FLORES-MENDEZ, an individual and AMBER COLLINS, an individual, and on behalf of classes of similarly situated individuals,

Plaintiffs,

v.

ZOOSK, INC., a Delaware corporation,

Defendant.

CASE NO: 4:20-cv-04929-WHA

PLAINTIFFS' SECOND AMENDED CLASS ACTION COMPLAINT FOR:

1. **NEGLIGENCE; AND**
2. **VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE § 17200, ET SEQ.**

DEMAND FOR A JURY TRIAL

Plaintiffs Juan Flores-Mendez, and Amber Collins, individually and on behalf of classes of similarly situated individuals (defined below), bring this action against Defendant Zoosk, Inc. ("Zoosk"). Plaintiffs and their counsel believe that reasonable discovery will provide additional evidentiary support for the allegations herein.

INTRODUCTION

1. Zoosk is a self-touted "leading online data company" with over 35 million members.[1] Zoosk employs its proprietary Behavioral Matchmaking™ technology to leverage the data generated by users on the platform and deliver matches which are predicted to result in "mutual attraction."[2]

2. To engage Defendant's online matchmaking services, customers create and populate user profiles with personally identifiable information ("PII") such as first and last name, email address, password, home address, telephone number, and payment card information. Zoosk customers trust that their PII will be maintained in a secure manner and kept from unauthorized disclosure to third parties as outlined in Zoosk's Privacy Policy.[3]

3. Zoosk customers also have the option of paying for a premium subscription service, which costs $29.99 for a single month, or $12.49 per month for a six-month period. Plaintiff Juan Flores-Mendez paid for this subscription before the Data Breach was announced.

4. Over the first two weeks of May, a group calling itself the "ShinyHunters" went on a hacking rampage and subsequently set out to hawk what it claimed to be close to 200 million stolen records from at least 13 companies, including "Zoosk."[4] Indeed, of all the companies targeted, Zoosk had the largest breach, as the cybercriminals grabbed 30 million user records.[5]

---

[1] https://about.zoosk.com/en/about/

[2] https://www.sec.gov/Archives/edgar/data/1438964/000119312514146003/d672159ds1.htm

[3] https://docviewer.zoosk.com/legal-privacy-en_eu.html

[4] https://www.wired.com/story/shinyhunters-hacking-group-data-breach-spree/

[5] https://www.dailymail.co.uk/sciencetech/article-8308167/Hacker-group-ShinyHunters-sells-73-MILLION-user-records-dark-web.html

5. An entity claiming to be a member of ShinyHunters said in an instant message conversation with WIRED that it is "not too hard" to breach so many organizations.[6]

6. According to its notice to affected customers, on May 11, 2020 Zoosk "learned that an unknown third party claimed to have accessed certain Zoosk member information" (the "Data Breach.").

7. Over three weeks later, and more than four weeks after the Data Breach occurred, Zoosk notified affected customers that their PII had been disclosed to unauthorized and malicious third parties.

8. To date, Zoosk has acknowledged that the customer information disclosed in the Data Breach included a combination of the following PII:

- name;
- email address;
- date of birth;
- generalized demographical information;
- gender;
- gender search preferences; and
- password information.

9. Zoosk's Notice of Data Security Event was sent via email on May 28, 2020, including a phone number for customer inquiries, as required by Cal. Civ. Code section 1798.82(a). Section 1798.82(a) requires businesses to notify "any California resident (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or

---

[6] https://www.wired.com/story/shinyhunters-hacking-group-data-breach-spree/

security credential could render that personal information readable or usable. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system."

10. The Zoosk customer PII disclosed in the Data Breach is protected by the California Consumer Privacy Act of 2018 ("CCPA"), which went into effect on January 1, 2020. For purposes of the CCPA, "personal information" is defined as an individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (1) social security number; (2) driver's license number or California ID card number; (3) account number or credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account; (4) medical information; and/or (5) health insurance information.

11. Alternatively, protected PII includes "A username of email address in combination with a password or security questions and answer that would permit access to an online account."

12. According to Zoosk's notice to affected customers, the PII subjected to unauthorized access and exfiltration, theft or disclosure in the Data Breach includes (among other things): (i) customers' unencrypted and unredacted name, and (ii) an email address that serves as an account login/account number, and (iii) password (although not confirmed at the time of the notice). In combination, those pieces of PII could permit access to other accounts using similar passwords, including financial accounts.

13. Zoosk has failed to maintain reasonable security controls and systems appropriate for the nature of the PII it maintains as required by the CCPA and other common and statutory laws.

14. Zoosk also failed to maintain proper measures to detect hacking and intrusion. According to its notice to affected customers, Zoosk did not learn that its customer records were stolen until the hack was publicly reported. As explained below, Zoosk should have had breach detection protocols in place. If it had, it could have learned of the breach and alerted customers much sooner.

15. Because (i) Zoosk has failed to maintain reasonable security measures, and (ii) the names that Zoosk disclosed in combination with emails and passwords were unredacted and unencrypted, Zoosk has breached its legal duties and obligations to Plaintiffs and Class Members.

16. Zoosk claims its "investigation remains ongoing," is "taking several steps to monitor systems and enhance our existing security measures and processes," but the viewing, theft, and attempted sale of California consumers' PII on the dark web has already occurred and cannot be cured.

17. Defendant disregarded Plaintiffs' and Class members' privacy rights in the PII by, among other things, (i) failing to implement reasonable security safeguards to prevent or timely detect the Data Breach; (ii) failing to disclose to customers that it did not implement such reasonable security safeguards; and (iii) failing to provide sufficiently prompt, thorough, and accurate notice and information concerning the Data Breach.

18. As a result of the Data Breach, Plaintiffs and the Classes have been injured in several ways. Plaintiffs and Class members (i) now know or should know that their PII was hacked and put up for sale on the dark web for purchase by malicious actors; (ii) face an imminent and ongoing risk of identity theft and similar cybercrimes; (iii) have expended and will continue to expend time and money to protect against cybercrimes; (iv) have lost value in their PII; and (v) did not receive the benefit of their bargain with Defendant regarding data privacy.

19. Plaintiffs and Class members are therefore (i) entitled to actual damages under the CCPA and other laws, (ii) have incurred actual and concrete damages as a result of the unauthorized sale of their PII to malicious actors on the dark web, and (iii) face ongoing risks of disclosure of their PII in subsequent data breaches because Defendant has not demonstrated that it has implemented reasonable security systems and procedures. Plaintiffs and Class members have a significant interest in the protection and safe storage of their PII. They are therefore entitled to declaratory, injunctive, and other equitable relief necessary to protect their PII. This includes, but is not limited to, an order compelling Defendant to adopt reasonable security procedures and practices to safeguard customers' PII and prevent future data breaches.

JURISDICTION AND VENUE

20. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 class members, and one or more members of the Classes are residents of a different state than Defendant Zoosk. The Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

21. This Court has personal jurisdiction over Defendant because it has continuous and systematic contacts with and conduct substantial business in the State of California and this District. Defendant Zoosk maintains its principal place of business in this District and has continuous and systematic contacts with and conducts substantial business in the State of California and this District.

22. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b). A substantial part of the events giving rise to these claims took place in this District, numerous Class members reside in this District and were therefore harmed in this District.

INTRADISTRICT ASSIGNMENT

23. This action is properly assigned to the San Francisco Division of this District pursuant to N.D. Cal. L.R. 3-2 because a substantial part of the events or omissions giving rise to Plaintiffs' claims arose in the counties served by the San Francisco Division. Zoosk is headquartered in this Division and conducts substantial business in the counties served by this Division, has marketed, advertised, sold, and collected contact information from consumers in this District, and has caused harm to Class members residing in those counties.

PARTIES

24. Plaintiff Juan Flores-Mendez ("Plaintiff Flores-Mendez") is a permanent resident of, California. Plaintiff Flores-Mendez created a user profile on Zoosk's website in or about 2015 or 2016. Plaintiff Flores-Mendez entrusted Zoosk with their PII. On May 28, 2020, Plaintiff Flores-Mendez received a notice in the mail from Zoosk notifying him that his PII had been accessed by malicious third parties without authorization. Because of the Data Breach, he has continuously monitored his various accounts to detect misuse of his PII and will continue to expend time to protect against fraudulent use or sale of his PII.

25. As a result of the notice, Plaintiff Flores-Mendez spent time dealing with the consequences of the data breach, which includes time spent reviewing the account compromised by the breach, contacting his credit card company, reviewing her credit report for suspicious activity, putting fraud alerts on his credit report, exploring credit monitoring options, and self-monitoring his accounts.

26. Knowing that the hacker stole his PII, and that his PII may be available for sale on the dark web, has caused Plaintiff Flores-Mendez anxiety. Plaintiff Flores-Mendez is now greatly concerned about credit card theft and identity theft in general. This breach has given Plaintiff Flores-Mendez hesitation about utilizing online websites.

27. Plaintiff Amber Collins ("Plaintiff Collins") is a permanent resident of Simi Valley, California. Plaintiff Collins created a user profile on Zoosk's website in or about 2016. Plaintiff Collins entrusted Zoosk with their PII. During the first week of June, 2020, an alert notice from Credit Karma notifying her of the breach of her Zoosk account. Because of the Data Breach, Plaintiff Collins has continuously monitored her various accounts to detect misuse of her PII and will continue to expend time to protect against fraudulent use or sale of her PII.

28. As a result of the notice, Plaintiff Collins spent time dealing with the consequences of the data breach, which includes time spent reviewing the account compromised by the breach, contacting her credit card company, signing up for credit monitoring options, reviewing her credit report for suspicious activity, putting fraud alerts on her credit reports, and self-monitoring her accounts.

29. Knowing that the hacker stole her PII, and that her PII may be available for sale on the dark web, has caused Plaintiff Collins anxiety. Plaintiff Collins is now greatly concerned about credit card theft and identity theft in general. This breach has given Plaintiff Collins has hesitation about Zoosk and other online websites.

30. Defendant Zoosk is a for-profit Delaware corporation and maintains a headquarters and principal place of business in San Francisco, California. The Zoosk app, available in more than 80 countries, is a free download, but charges users who want to send messages and chat with other subscribers, similar to Match. Zoosk has gross revenues in excess of $25 million as adjusted. Zoosk

was acquired by Berlin-based Spark Networks in July 2019. The deal valued Zoosk at approximately $258 million.

31. According to data from Sensor Tower, Zoosk has generated worldwide in-app revenue of $250 million and has seen 38 million downloads since January 2014. Half of those downloads (19 million) are from the U.S., which also accounts for $165 million (66%) of the revenue. In Quarter one of 2019, Zoosk had revenue of $13 million.

FACTUAL BACKGROUND

Defendant's Relevant Privacy Policies

32. Personal data must be provided in order for consumers to use the service provided by Zoosk.

33. Zoosk's Privacy Policy is available on its website and provides customers with terms and conditions regarding the treatment of their PII. For example, it states:

> When you register, use or subscribe to any of our Services or take part in any interactive features of the Services (such as any contests, games, promotions, quizzes, surveys, research or other services or features), we may collect a variety of information, including:
>
> a. Contact Information such as your name, email address, phone number, and address ("Contact Information");
> b. Sensitive Information such as race, ethnicity, sexual preferences and experiences, political affiliation, religious affiliation, union memberships, or any biometric information you provide through the use of our Services (your "Sensitive Personal Data");
> c. Other Information such as birth date, videos, passwords, billing information, credit card information, demographic information, place of work or education, your personal interests and background, gender, age, dating age range preference, physical characteristics, personal description, life experiences, geographic location, your photos and any information derived from them, and any other information you share with the Services. We may collect billing or payments information if you engage with a paid Service.[7]

34. Additionally, Zoosk collects information about:[8]

- How consumers use the service (*i.e.*, pages and profiles viewed);

[7] https://docviewer.zoosk.com/legal-privacy-en.html

[8] *Id.*

- Content users upload (*i.e.*, time, date and place information for photos uploaded to the site as well as the identity of those to whom the photos are shared);
- Information about your devices (*i.e.*, model and manufacturer, mobile carrier, phone number, other apps downloaded, IP address, browser type, Internet service provider, platform type, the site from which you came and the site to which you are going when you leave our website);
- Communications (sent directly to Zoosk or comments made by users on third-party services such as Twitter Instagram, Pinterest, Tumblr and YouTube);
- Information taken from social networking sites (i.e. IP address, browser type, Internet service provider, platform type, the site from which you came and the site to which you are going when you leave our website, date and time stamp and one or more cookies that may uniquely identify your browser or your account);
- Location data;
- User's address book contact information; and
- Aggregated data.

35. Zoosk's Privacy Policy assures Zoosk customers their PII is secure. For example, Zoosk states it "At Zoosk, we value your privacy and trust" and "work[s] with third parties to employ technologies…to ensure the safety and security of your data…"[9]

Zoosk Uses PII to Maximize Its Profits and For Marketing and

36. Zoosk's Privacy Policy reveals the significant benefit Zoosk derives from collecting and maintaining its customers PII. In addition to the uses listed above, Zoosk:

- Permits third party advertising networks, social media companies and other third party businesses to collect PII (including Internet/Network Information, Commercial Information, and Inferences) directly from consumer's browsers or devices through cookies or tracking technologies. These third parties use this information for the purposes of serving ads, for ad campaign measurement and

[9] *Id.*

analytics, and may sell that information to other businesses for advertising and other purposes;

- Uses PII to facilitate users' purchase of subscriptions and premium add-ons;
- Shares PII with promotional partners to provide contests and sweepstakes or other joint promotional activities;
- May utilize PII in connection with any company transaction, such as a merger, sales of assets or shares, reorganization, financing, change of control or acquisition of all or a portion of our business by another company or third party or in the event of bankruptcy, dissolution, divestiture or any related or similar proceedings for marketing and advertising purposes; and
- Uses PII to monitor, improve, and develop its products and services.

Zoosk Failed to Take Reasonable Steps to Protect User Data

37. By collecting, using, and deriving significant benefit from customers' PII, Zoosk had a legal duty to take reasonable steps to protect this information from disclosure.

38. As discussed below, Defendant also had a legal duty to take reasonable steps to protect customers' PII under applicable federal and state statutes, including Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which is further defined by federal and state guidelines and industry norms.

39. Defendant breached its duties by failing to implement reasonable safeguards to ensure Plaintiffs' and Class members' PII was adequately protected. As a direct and proximate result of this breach of duty, the Data Breach occurred, and Plaintiffs and Class members were harmed. Plaintiffs and Class members did not consent to having their PII disclosed to any third-party, much less a malicious hacker who would sell it on the dark web.

40. The Data Breach was a reasonably foreseeable consequence of Defendant's inadequate security systems. Defendant Zoosk, is valued at $258 Million Dollars, has the resources to implement reasonable security systems to prevent or limit damage from data breaches. Even so, it failed to properly invest in its data security. If Zoosk had implemented reasonable data security systems and procedures (*i.e.*, followed guidelines from industry experts and state and federal

governments), then it likely could have prevented hackers from infiltrating its systems and accessing its customers' PII.

Zoosk's Failure to Take Reasonable Steps to Protect User Data Resulted in a Massive Data Breach

41. A data breach is any incident where confidential or sensitive information has been accessed without permission. Breaches are the result of a cyberattack where criminals gain unauthorized access to a computer system or network and steal the private, sensitive, or confidential personal and financial data of the customers or users contained within.

42. Despite these assurances and the significant benefit Zoosk receives by collecting and maintaining its customers' PII, Zoosk did not adopt reasonable data measures and systems to protect customers' PII or prevent and detect unauthorized access to this data. Zoosk maintains a business that operates exclusively online and collects hundreds of millions of dollars from online customers each year; it has the resources to adopt reasonable protections and should have known to do so. It knew or should have known that its systems had inadequate protections that placed its customers at significant risk of having their PII stolen by hackers.

43. Such failures resulted in the hack orchestrated by ShinyHunters on January 12, 2020 which resulted in the theft of 30 million account credentials.

44. Despite its mammoth scope, Zoosk, did not become aware of the breach until May 11, 2020 – nearly four months later. Such timing coincided with media reports of the sale of such information by ShinyHunters on the dark web for $500 "a pop."[10]

Zoosk Did Not Notify Affected Consumers Within a Reasonable Time

45. Defendant also had a duty to timely discover the Data Breach and notify Plaintiffs and Class members that their PII had been compromised. Defendant breached this duty by failing to use reasonable intrusion detection measures to identify the Data Breach when it occurred months prior, and then, promptly upon learning of the breach.

[10] https://www.cshub.com/attacks/articles/iotw-shiny-hunters-is-the-new-threat-actor-in-town

46. Zoosk notified Plaintiffs and the members of the classes that personal information stolen during the breach included names, email addresses, and passwords.

Annual Monetary Losses from Identity Theft are in the Billions of Dollars in Value of Personally Identifiable Information

47. Zoosk's failure to implement reasonable security systems has caused Plaintiffs and Class members to suffer and continue to suffer harm that adversely impact Plaintiffs and Class members economically, emotionally, and/or socially. As discussed above, Plaintiffs and Class members now face an imminent and ongoing threat of identity theft and resulting harm. These individuals now must spend significant time and money to continuously monitor their accounts and credit scores to limit potential adverse effects of the Data Breach regardless of whether any Class member ultimately falls victim to identity theft.

48. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Experion has created the below chart tracking the sale process of the most common pieces of hacked information.[11]

49. Such figures are consistent with those reported by other media outlets.

50. The information stolen from Zoosk included usernames and passwords—PII that is highly valued among cyber thieves and criminals on the Dark Web. For example, Apple ID usernames and passwords were sold on average for $15.39 each on the Dark Web, making them the most valuable non-financial credentials for sale on that marketplace. Usernames and passwords for eBay ($12), Amazon (≤$10), and Walmart (≤$10) fetch similar amounts.[12]

51. This is particularly problematic because password reuse and modification is a very common behavior (observed on 52% of users in one study and far more in current polls).[13] By

[11] https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-sellingfor-on-the-dark-web/

[12] Don Reisinger, *Here's How Much Your Stolen Apple ID Login Costs on the Dark Web,* Fortune (March 7, 2018), https://fortune.com/2018/03/07/apple-id-dark-web-cost/; *See also* https://www.npr.org/2018/02/22/588069886/take-a-peek-inside-the-market-for-stolen-usernames-andpasswords.

[13] The Next Domino To Fall: Empirical Analysis of User Passwords across Online Services Chun Wang, Steve T.K. Jan, Hang Hu, Douglas Bossart, Gang Wang. In Proceedings of The ACM

unlawfully obtaining this information, cyber criminals can use these credentials to access other services beyond that which was hacked.

52. There may be a time lag between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[14]

53. As a result of the Data Breach, Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and Class Members are also subject to a higher risk of phishing and pharming where hackers exploit information they already obtained in an effort to procure even more PII. Plaintiff and Class Members are presently incurring and will continue to incur such damages, in addition to any fraudulent credit and debit card charges incurred by them, and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies. In addition, Plaintiff and Class Members now run the risk of unauthorized individuals creating credit cards in their names, taking out loans in their names, and engaging in other fraudulent conduct using their identities.

54. Despite this harm, Zoosk has failed to recognize the impact of the Data Breach on its customers; it has not even offered impacted customers credit monitoring services or other mitigation measures beyond what is available to the public. For example, Zoosk's notice to affected customers puts the onerous on the user to change his password and states that they "are providing the contact details for the national consumer reporting agencies and a reminder to remain vigilant for incidents

---

Conference on Data and Applications Security and Privacy (CODASPY). Tempe, AZ, March 2018.

[14] See GAO, Report to Congressional Requesters, at 33 (June 2007), *available at* *http://www.gao.gov/new.items/d07737.pdf*

for fraud and identity theft by reviewing account statements and monitoring credit reports.

55. Due to Defendant's conduct, Plaintiffs and Class members are entitled to credit monitoring. Credit monitoring is reasonable here. The PII taken can be used towards identity theft and other types of financial fraud against the Class members. There is no question that this PII was taken by sophisticated cybercriminals, increasing the risks to the Class members. The consequences of identity theft are serious and long-lasting. There is a benefit to early detection and monitoring.

56. Annual subscriptions for credit monitoring plans range from approximately $219 to $329 per year.

57. Plaintiffs and Class members therefore have a significant and cognizable interest in obtaining equitable relief (in addition to any monetary damages) that protects them from these long-term threats.

CLASS ACTION ALLEGATIONS

58. Plaintiffs bring this nationwide class action pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following classes:

Nationwide Class: All individuals whose PII was compromised in the Data Breach announced by Zoosk on June 3, 2020.

California Subclass: All individuals whose PII was compromised in the Data Breach announced by Zoosk on June 3, 2020, who reside in California.

Subscription Subclass: All individuals whose PII was compromised in the Data Breach announced by Zoosk on June 3, 2020, who paid for subscriptions with Zoosk.

59. Specifically excluded from this Class are Defendant; the officers, directors, or employees of Defendant; any entity in which Defendant has a controlling interest; and any affiliate, legal representative, heir, or assign of Defendant. Also excluded are any federal, state, or local governmental entities, any judicial officer presiding over this action and the members of his/her immediate family and judicial staff, and any juror assigned to this action.

60. Plaintiffs reserve the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

61. **Numerosity:** The Classes are sufficiently numerous, as each includes hundreds of thousands of individuals. According to the Notice provided by Zoosk, there are 560,138 California residents affected. Thus, joinder of such persons in a single action or bringing all members of the Classes before the Court is impracticable for purposes of Rule 23(a)(1).

62. The question is one of a general or common interest of many persons and it is impractical to bring them all before the Court. The disposition of the claims of the members of the Classes in this class action will substantially benefit both the parties and the Court.

63. **Commonality:** There are questions of law and fact common to each Class for purposes of Rule 23(a)(2), including:

a. Whether and when Defendant actually learned of the data breach and whether its response was adequate;

b. Whether Defendant owed a duty to the Class to exercise due care in collecting, storing, safeguarding and/or obtaining their PII;

c. Whether Defendant breached that duty;

d. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiffs' and Class members' PII;

e. Whether Defendant acted negligently in connection with the monitoring and/or protecting of Plaintiff's and Class members' PII;

f. Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiffs' and Class members' PII secure and prevent loss or misuse of that PII;

g. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the data breach to occur;

h. Whether Defendant caused Plaintiffs and Class members damages, including compensatory, statutory, actual, consequential, or nominal damages;

i. Whether Defendant violated the law by failing to promptly notify class members that their PII had been compromised;

j. Whether Plaintiffs and the other Class members are entitled to credit monitoring and other monetary relief;

k. Whether Plaintiffs and Class members are entitled to compensatory, statutory, actual, consequential, or nominal damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct; and

l. Whether Defendant violated California's Deceptive and Unfair Trade Practices Act by failing to implement reasonable security procedures and practice.

64. **Typicality:** Plaintiffs assert claims that are typical of the claims of each respective Class for purposes of Rule 23(a)(3). Plaintiffs and all members of each respective Class have had their PII compromised as a result of the data breach and Defendant's misconduct.

65. **Adequacy:** Plaintiffs will fairly and adequately represent and protect the interests of the other members of each respective Class for purposes of Rule 23(a)(4). Plaintiffs have no interests antagonistic to those of other members of each respective Class. Plaintiffs are committed to the vigorous prosecution of this action and has retained counsel experienced in litigation of this nature to represent her. Plaintiffs anticipate no difficulty in the management of this litigation as a class action.

66. Class certification is appropriate under Rule 23(b)(2) because Defendant has acted on grounds that apply generally to each Class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting each Class as a whole.

67. Class certification is appropriate under Rule 23(b)(3) because common questions of law and fact substantially predominate over any questions that may affect only individual members of each Class.

68. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by the members of each respective Class. Similar or identical statutory and common law violations and deceptive business practices are involved. Individual questions, if any, pale by comparison to the numerous common questions that predominate.

69. The injuries sustained by Plaintiffs and the members of each Class flow, in each instance, from a common nucleus of operative facts – Defendant's misconduct.

70. Plaintiffs and the members of each Class have been damaged by Defendant's misconduct.

71. Proceeding as a class action provides substantial benefits to both the parties and the Court because this is the most efficient method for the fair and efficient adjudication of the controversy. Members of each Class have suffered and will suffer irreparable harm and damages as a result of Defendant's wrongful conduct. Because of the nature of the individual claims of the members of each Class, few, if any, could or would otherwise afford to seek legal redress against Defendant for the wrongs complained of herein, and a representative class action is therefore the appropriate, superior method of proceeding and essential to the interests of justice insofar as the resolution of claims of the members of each Class is concerned. Absent a representative class action, members of each Class would continue to suffer losses for which they would have no remedy, and Defendant would unjustly retain the proceeds of its ill-gotten gains. Even if separate actions could be brought by individual members of each Class, the resulting multiplicity of lawsuits would cause undue hardship, burden, and expense for the Court and the litigants, as well as create a risk of inconsistent rulings, which might be dispositive of the interests of the other members of each Class who are not parties to the adjudications and/or may substantially impede their ability to protect their interests.

72. Particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and the Class members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiffs and the Class members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach; and

e. Whether Class members are entitled to compensatory, statutory, actual, consequential, or nominal damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

FIRST CAUSE OF ACTION

NEGLIGENCE

(By Plaintiffs and the Classes)

73. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 72 above.

74. Defendant owed Plaintiffs and Class members a duty to exercise reasonable care in protecting their PII from unauthorized disclosure or access. Defendant breached its duty of care by failing to implement reasonable security procedures and practices to protect Plaintiffs' and Class members' PII. Defendant failed to, inter alia: (i) implement security systems and practices consistent with federal and state guidelines; (ii) implement security systems and practices consistent with industry norms; (iii) timely detect the Data Breach; and (iv) timely disclose the Data Breach to impacted customers.

75. Additionally, Defendant collected money from the Subscription Subclass but failed to commit appropriate portions of that money to enact security measures to protect Plaintiffs' and Class Members' PII.

76. Defendant knew or should have known Plaintiffs' and Class members' PII was highly sought after by hackers and that Plaintiffs and Class members would suffer significant harm if their PII was stolen by hackers.

77. Defendant also knew or should have known that timely disclosure of the Data Breach was required and necessary to allow Plaintiffs and Class members to take appropriate actions to mitigate the resulting harm. These efforts include, but are not limited to, freezing accounts, changing passwords, monitoring credit scores/profiles for fraudulent charges, contacting financial institutions,

and cancelling or monitoring government-issued IDs such as passports and driver's licenses. The risk of significant harm to Plaintiffs and Class members (including identity theft) increased as the amount of time between the Data Breach and disclosure lengthened to reach a full twenty-two days.

78. Defendant had a special relationship with Plaintiffs and the Class members who entrusted Defendant with several pieces of PII. Customers were required to provide PII when utilizing Defendant's properties and/or services. Plaintiffs and Class members were led to believe Defendant would take reasonable precautions to protect their PII and would timely inform them if their PII was compromised, but the Defendant did not do so.

79. Defendant's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45(a).

80. The Federal Trade Commission ("FTC") has established security guidelines and recommendations to help entities protect PII and reduce the likelihood of data breaches.

81. Specifically, Section 5 of the FTC Act, 15 U.S.C. § 45(a), prohibits "unfair … practices in or affecting commerce," including, as interested and enforced by the FTC, the unfair practices of failing to use reasonable measures to protect PII by companies such as Defendant.

82. Various FTC publications and data security breach orders further form the basis of Defendant's duty.[15] Plaintiffs and Class members are consumers under the FTC Act. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with industry standards.

83. In addition, Cal. Civ. Code § 1798.81.5 requires Defendant to take reasonable steps and employ reasonable methods of safeguarding the PII of Class members who are California residents.

84. Defendant violated the FTC Act and the CCPA by failing to use reasonable security measures to protect PII and not complying with applicable industry, federal, and state guidelines

[15] See, e.g., Data Protection: Actions taken by Equifax and Federal Agencies in Response to the 2017 Breach, United States Government Accountability Office (Aug. 30, 2019), available at: https://www.gao.gov/products/GAO-18-559 (regarding the Equifax data breach).

and standards. Defendant's conduct was particularly unreasonable given the nature and amount of customer PII it stored and the foreseeability and resulting consequences of a data breach.

85. Plaintiffs and Class members are part of the Class of persons the FTC Act and CCPA were intended to protect. The harm that was proximately caused by the Data Breach is the type of harm the FTC Act and CCPA were intended to guard against. The FTC has brought enforcement actions against entities that, due to a failure to employ reasonable data security measures, caused the same harm as that suffered by Plaintiffs and Class members here.

86. As a result of Defendant's negligence, Plaintiffs and Class members suffered injuries that may include: (i) the lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the data breach, including but not limited to time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised account; (iv) the continued risk to their PII, which remains for sale on the dark web and is in Defendant's possession, subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of customers and former customers in its continued possession; (v) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the PII compromised as a result of the data breach for the remainder of the lives of Plaintiffs and Class members, including ongoing credit monitoring.

87. The harm that Plaintiffs and Class members suffered (and continue to suffer) was the reasonably foreseeable product of Defendant's breach of its duty of care. Defendant failed to enact reasonable security procedures and practices and Plaintiffs and Class members were the foreseeable victims of data theft that exploited the inadequate security measures. The PII accessed in the Data Breach is precisely the type of information that hackers seek and use to commit cyber crimes.

///

///

///

///

SECOND CAUSE OF ACTION

VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW

CAL. BUS. & PROF. CODE § 17200 – UNLAWFUL BUSINESS PRACTICES

(By Plaintiffs and the Classes)

88. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 87 above.

89. Defendant's conduct as alleged herein constitutes unlawful, unfair, and/or fraudulent business acts or practices as prohibited by the UCL.

90. Defendant engaged in business acts and practices deemed "unlawful" under the UCL, because, as alleged above, Defendant violated the FTC Act and failed to protect Plaintiffs' and Class Members' PII.

91. "Unfair" acts under the UCL have been interpreted using three different tests: (1) whether the public policy which is a predicate to a consumer unfair competition action under the unfair prong of the UCL is tethered to specific constitutional, statutory, or regulatory provisions; (2) whether the gravity of the harm to the consumer caused by the challenged business practice outweighs the utility of the defendant's conduct; and (3) whether the consumer injury is substantial, not outweighed by any countervailing benefits to consumers or competition, and is an injury that consumers themselves could not reasonably have avoided. Defendant's conduct is unfair under each of these tests.

92. Defendant engaged in business acts or practices deemed "unfair" under the UCL because, as alleged above, Defendant failed to disclose the inadequate nature of the security of its computer systems and networks that stored Plaintiffs' and Class members' sensitive PII. *See* Cal. Bus. & Prof. Code § 17200.

93. Additionally, Defendant collected money from the Subscription Subclass but failed to commit appropriate portions of that money to enact security measures to protect Plaintiffs' and Class Members' PII.

94. Defendant's conduct was also unfair because it failed to use reasonable security measures to protect Plaintiffs' and Class Members' PII.

95. Defendant's conduct violates the policies of the statutes referenced above. Moreover, Defendant's conduct is contrary to public policy, immoral, unethical, oppressive, unscrupulous and/or substantially injurious to consumers. Among other things, it is contrary to the public policy in favor of protecting consumer data.

96. The gravity of the harm of Defendant's failure to secure and protect Plaintiffs' and Class Members' sensitive PII is significant and there is no corresponding benefit resulting from such conduct. Finally, because Plaintiffs and Class Members were completely unaware of Defendant's inadequate information security practices, they could not have avoided the harm resulting from Defendant's conduct.

97. Had Plaintiffs known that their PII would not be adequately secured and protected, they would not have used Defendant's services. Plaintiffs and Class Members have a property interest in their sensitive PII. By failing to adequately secure and protect that sensitive PII, Defendant has taken property from Plaintiffs and Class Members without providing just or any compensation.

98. Plaintiffs and Plaintiff and Class members have lost money and property as a result of Defendant's conduct in violation of the UCL and seek restitution on behalf of themselves and Class Members. Additionally, Plaintiffs individually and on behalf of the Class, seek an injunction enjoining Defendant from engaging in the unlawful conduct alleged in this claim and requiring Defendant to delete Plaintiff's and Class members' sensitive PII, to cease further collection of Plaintiff's and Class members' sensitive PII, and other appropriate equitable relief, including but not limited to implementing adequate information security policies and practices.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Classes, request the following relief:

1. A determination that this action is a proper class action under Federal Rule of Civil Procedure 23, certifying the Classes, and appointing Plaintiffs as Class Representatives and their counsel as Class Counsel;
2. Finding that Defendant's conduct was unlawful as alleged herein;

3. An award of compensatory, punitive, statutory, actual, consequential, or nominal damages or civil penalties to Plaintiffs and the Classes as warranted by applicable law;
4. An order requiring Defendant to purchase or provide funds for credit monitoring services for Plaintiffs and all Class Members;
5. An award of injunctive or other equitable relief that directs Defendant to implement adequate security procedures and practices to protect customers' PII that conform to relevant federal and state guidelines and industry norms;
6. Awarding Plaintiffs and the Class reasonable costs and expenses incurred in this action, including attorneys' fees, costs, and expenses, including expert fees;
7. Awarding Plaintiffs and the Class Members pre- and post-judgment interest; and
8. Such other relief as the Court may deem just and proper.

Dated: July 28, 2021

By: /s/ Kiley L. Grombacher
Kiley L. Grombacher

BRADLEY/GROMBACHER, LLP
Marcus J. Bradley, Esq. (SBN 174156)
Kiley L. Grombacher, Esq. (SBN 245960)
Lirit A. King, Esq. (SBN 252521)
31365 Oak Crest Drive, Suite 240
Westlake Village, California 91361
Telephone: (805) 270-7100
Facsimile: (805) 270-7589
E-Mail: mbradley@bradleygrombacher.com
kgrombacher@bradleygrombacher.com
lking@bradleygrombacher.com

BRADLEY/GROMBACHER, LLP
Robert N. Fisher (SBN 302919)
477 Madison Avenue, Suite 6000
New York, NY 10022
Telephone: (805) 270-7100
E-Mail: rfisher@bradleygrombacher.com

CROSNER LEGAL P.C.
Zachary M. Crosner (SBN 272295)
Michael R. Crosner (SBN 41299)
433 N. Camden Dr., Suite 400
Beverly Hills, CA 90210
Telephone: (310) 496-4818
Facsimile: (310) 510-6429
Email: zach@crosnerlegal.com
mike@crosnerlegal.com

MORGAN & MORGAN
COMPLEX LITIGATION GROUP
John A. Yanchunis (*admitted pro hac vice*)
Ryan McGee (*admitted pro hac vice*)
201 N Franklin St., 7th Floor
Tampa, FL 33602
Telephone: (813) 223-5505
Email: jyanchunis@forthepeople.com
rmcgee@forthepeople.com

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial for all claims so triable.

Dated: July 28, 2021

By: /s/ Kiley L. Grombacher
Kiley L. Grombacher

BRADLEY/GROMBACHER, LLP
Marcus J. Bradley, Esq. (SBN 174156)
Kiley L. Grombacher, Esq. (SBN 245960)
Lirit A. King, Esq. (SBN 252521)
31365 Oak Crest Drive, Suite 240
Westlake Village, California 91361
Telephone: (805) 270-7100
Facsimile: (805) 270-7589
E-Mail: mbradley@bradleygrombacher.com
kgrombacher@bradleygrombacher.com
lking@bradleygrombacher.com

BRADLEY/GROMBACHER, LLP
Robert N. Fisher (SBN 302919)
477 Madison Avenue, Suite 6000
New York, NY 10022
Telephone: (805) 270-7100
E-Mail: rfisher@bradleygrombacher.com

CROSNER LEGAL P.C.
Zachary M. Crosner (SBN 272295)
Michael R. Crosner (SBN 41299)
433 N. Camden Dr., Suite 400
Beverly Hills, CA 90210
Telephone: (310) 496-4818
Facsimile: (310) 510-6429
Email: zach@crosnerlegal.com
mike@crosnerlegal.com

Attorneys for Plaintiffs
[Additional counsel on following page]

MORGAN & MORGAN
COMPLEX LITIGATION GROUP
John A. Yanchunis (*admitted pro hac vice*)
Ryan McGee (*admitted pro hac vice*)
201 N Franklin St., 7th Floor
Tampa, FL 33602
Telephone: (813) 223-5505
Email: jyanchunis@forthepeople.com
rmcgee@forthepeople.com